What is claimed is:

Sub B1

1. A method of handling network packets, comprising:

receiving encrypted network packets from the network at a network interface computer; and

passing the encrypted network packets to a computer on an internal network.

2. The method of claim 1, further comprising, before passing the encrypted network packets to the computer on the internal network:

determining a destination computer for each encrypted network packet.

3. The method of claim 2, wherein determining further includes:

determining whether a source computer that sent each encrypted network packet is authorized to send encrypted network packets to the destination computer.

4. The method of claim 2, wherein determining includes:

examining a field in a header of the network packet.

5. The method of claim 4, wherein the field corresponds to a virtual network tunnel.

6. The method of claim 2, wherein an encrypted network packet is passed to the computer on the internal network when the destination computer for the encrypted network packet is determined to be the computer on the internal network.

Sub B2

7. The method of claim 1, further comprising:

decrypting an encrypted network packet at the network interface computer when the destination computer for the encrypted network packet is determined to be the network interface computer.

8. The method of claim 7, further comprising:

passing the decrypted network packet to the computer on the internal network.

9. The method of claim 1, further comprising:

encrypting network packets; and

sending encrypted network packets from the network interface computer to the network.

10. The method of claim 9, wherein the computer on the internal network encrypts the network packets, and further comprising:

passing the encrypted network packets to the network interface computer.

11. The method of claim 1, wherein the network interface computer comprises a firewall computer.

12. The method of claim 1, wherein the network comprises a public network.

13. A method of handling network packets, comprising:

receiving encrypted network packets at a first computer over a network from a second computer;

examining a field in each network packet to determine which of a plurality of encryption algorithms was used to encrypt the network packet; and

decrypting the network packet in accordance with the determined encryption algorithm.

14. The method of claim 13, further comprising:

examining the field to determine a destination computer for each encrypted network packet.

15. The method of claim 14, further comprising:

determining whether a source computer that sent each encrypted network packet is authorized to send encrypted network packets to the destination computer.

16. The method of claim 14, further comprising:

17

passing encrypted network packets to a computer on an internal network when the destination computer is determined to be the computer on the internal network.

17. The method of claim 14, further comprising:

decrypting network packets when the destination computer is determined to be the first computer.

18. The method of claim 17, further comprising:

passing the decrypted network packets to a computer on an internal network.

19. The method of claim 14, wherein the field corresponds to a virtual network tunnel.

20. The method of claim 14, wherein the network comprises a public network.

21. The method of claim 14, wherein the first computer comprises a firewall computer.

22. A method of handling network packets, comprising:

receiving network packets sent over a network;

determining which virtual tunnel each network packet was sent over; and

routing each network packet to a destination computer in accordance with the determined virtual tunnel.

23. The method of claim 22, further comprising:

decrypting each network packet in accordance with the determined virtual tunnel.

24. A method of handling network packets, comprising:

encrypting network packets at a computer connected to an internal network;

passing the encrypted network packet over the internal network to a public network interface computer; and

passing the encrypted network packet over a public network connected to the network interface computer.

25. A method of handling network packets, comprising:

receiving network packets sent over a network;

determining which virtual tunnel each network packet was sent over; and

determining whether a source computer that sent each network packet is authorized to send network packets to over the determined virtual tunnel.

26. The method of claim 25, further comprising:

routing each network packet to a destination computer in accordance with the determined virtual tunnel when the source computer is determined to be authorized.